(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－317734

(43)公開日　平成11年(1999)11月16日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ
			６２０Ａ
	６３０		６３０Ｃ

審査請求　未請求　請求項の数13　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－33760

(22)出願日　平成11年(1999) 2 月12日

(31)優先権主張番号　特願平10－31636

(32)優先日　平10(1998) 2 月13日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　宮▲崎▼　誠治
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

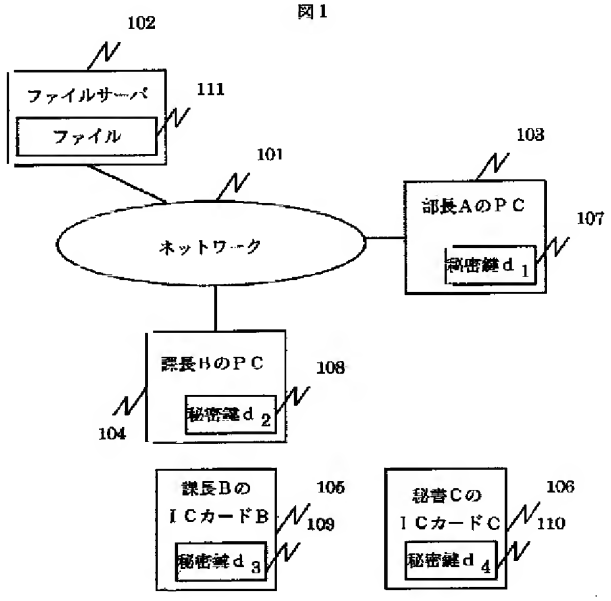
(54)【発明の名称】　データの暗号化復号化方法および、それを用いたネットワークシステム

(57)【要約】

【課題】(k,n)しきい値秘密分散法と楕円曲線暗号を組み合わせて、安全かつ高信頼なデータ管理システムを提供する。

【解決手段】秘密分散保持者が保有するデータを楕円曲線暗号における秘密鍵とし、(k,n)しきい値秘密分散法におけるしきい値ロジックは、各秘密分散保持者の秘密鍵と対を成す公開鍵を用いて計算する。この結果、情報を暗号化した後に、改めて秘密情報を分散させる必要が無くなり、分配者機関や分配者が必要なくなる。

図1



【特許請求の範囲】
【請求項１】(1)暗号化する時に：公開鍵暗号方法によって、秘密鍵(d_n)と公開鍵(Q_n)とをn組(nは正の整数)準備し、
少なくとも1つの前記公開鍵から新たな鍵を生成し、
前記新たな鍵と前記n個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(kはk≦nである正の整数)を準備し、
前記新たな鍵と前記n個の公開鍵を使用して、前記しきい値ロジックの計算を行い、
暗号化されたデータと前記しきい値ロジックの計算結果を保存し、
(2)復号化をする時に：前記n個の内のk個の秘密鍵と前記保存されたしきい値ロジックの計算結果から、前記しきい値ロジックに対応する値しきい値逆ロジックを使用して前記新たな鍵を復元し、
前記復元した鍵を使用して前記共通鍵暗号方法によって前記保存された暗号化データを復号化することを特徴とするデータの暗号化復号化方法。
【請求項２】請求項１に記載のデータの暗号化復号化方法であって、
前記公開鍵暗号方法は楕円曲線暗号であって、楕円曲線暗号に関係する定数(R)が前記暗号化データとともに保存され、復号化時に利用されることを特徴とするデータの暗号化復号化方法。
【請求項３】請求項１に記載のデータの暗号化復号化方法であって、
前記公開鍵から前記新たな鍵を生成する時に、ハッシュ関数を使用することを特徴とするデータの暗号化復号化方法。
【請求項４】請求項２に記載のデータの暗号化復号化方法であって、
前記楕円曲線暗号に関係する定数(R)は、楕円曲線のベースポイント(P)と乱数から計算され、
前記新たな鍵は前記公開鍵と該乱数から計算される値のハッシュ値であり、
前記しきい値ロジックは前記公開鍵と該乱数から計算される値のハッシュ値および前記新たな鍵を変数とする連立方程式を用いることを特徴とするデータの暗号化復号化方法。
【請求項５】請求項４に記載のデータの暗号化復号化方法であって、
前記新たな鍵を復号する時に、前記秘密鍵と前記定数を使用した計算結果のハッシュ値を前記しきい値逆ロジックで用いることを特徴とするデータの暗号化復号化方法。
【請求項６】請求項１に記載のデータの暗号化復号化方法であって、
(n-k)個以下の秘密鍵が使用不可能になった時は、
残りの少なくともk個の秘密鍵を使用して前記保存された暗号化データを復号し、
使用不可能な鍵またはすべての鍵に対して、秘密鍵と公開鍵を新たに用意し、
新しい公開鍵を使用して、再度復号化されたデータの暗号化を行うことを特徴とするデータの暗号化復号化方法。
【請求項７】ネットワークに接続され、それぞれ公開鍵暗号方法の秘密鍵を保管するn個(nは正の整数)の機器と、ネットワークに接続され前記複数の機器のいずれからもアクセス可能であり、前記秘密鍵に対応するすべての公開鍵を保管するサーバとを含むネットワークシステムであって、
データの暗号化を行う前記機器は、
少なくとも1つの前記公開鍵から新たな鍵を生成する手段と、
前記新たな鍵を使用して共通鍵暗号方法によってデータを暗号化する手段と、
前記新たな鍵と前記n個の公開鍵を使用して、前記新たな鍵と前記n個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(kはk≦nである正の整数)の計算を行う手段と、
暗号化されたデータと前記しきい値ロジックの計算結果を前記サーバに保存する手段を含み、
データの復号を行う前記機器は、
暗号化されたデータと前記しきい値ロジックの計算結果を前記サーバから読み出す手段と、
前記秘密鍵に関係し、前記しきい値ロジックに対応するしきい値逆ロジックの計算に必要なk個の値を前記機器から得る手段と、
前記読み出したしきい値ロジックの計算結果と前記得た値から、前記しきい値逆ロジックを使用して前記新たな鍵を復元する手段と、
前記復元した鍵を使用して前記共通鍵暗号方法によって前記読み出された暗号化データを復号化する手段を含むことを特徴とするネットワークシステム。
【請求項８】請求項７記載のネットワークシステムであって、
公開鍵暗号方法の秘密鍵を保管するn個の機器は、コンピュータ又は他の装置を介してネットワークに接続可能なICカードであることを特徴とするネットワークシステム。
【請求項９】請求項７記載のネットワークシステムであって、
前記公開鍵暗号方法は楕円曲線暗号であって、
前記暗号化装置において、
前記新たな鍵生成手段は、前記公開鍵と乱数から計算される値のハッシュ値を新たな鍵とし、前記公開鍵と乱数から計算される値のハッシュ値および前記新たな鍵を変数として前記しきい値ロジックの計算を行い、
前記暗号化機器の保存手段は、楕円曲線暗号に関係する

定数(R)を楕円曲線のベースポイント(P)と前記乱数から計算して前記暗号化データと共に保存し、
前記復号化機器において前記読み出し手段は、前記定数を読み出し、
前記得る手段は、前記秘密鍵と前記定数の計算結果のハッシュ値を得ることを特徴とするネットワークシステム。
【請求項１０】請求項９に記載のネットワークシステムであって、
前記復号化機器の前記得る手段は、前記秘密鍵を持つ他の機器に前記定数と共に前記秘密鍵のハッシュ処理要求を送信し、該他の機器から前記ハッシュ値を受信することを特徴とするネットワークシステム。
【請求項１１】請求項１０に記載のネットワークシステムであって、
前記機器の各々は、前記秘密鍵のハッシュ処理要求を受信する手段と、前記ハッシュ処理要求とともに送信されてきた前記定数と前記自機器内に保管している前記秘密鍵とを使用した計算結果のハッシュ処理を行う手段と、該ハッシュ値を該ハッシュ処理要求送信元に送信する手段とを持つことを特徴とするネットワークシステム。
【請求項１２】データの暗号化プログラムであって、
公開鍵暗号方法によって、秘密鍵(d_n)と公開鍵(Q_n)とをn組(nは正の整数)準備し、
少なくとも1つの前記公開鍵から新たな鍵を生成し、
前記新たな鍵を使用して共通鍵暗号方法によってデータを暗号化し、
前記新たな鍵と前記n個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(k≦nである正の整数)を準備し、
前記新たな鍵と前記n個の公開鍵を使用して、前記しきい値ロジックの計算を行い、
暗号化されたデータと前記しきい値ロジックの計算結果を保存することを特徴とするデータの暗号化プログラム。
【請求項１３】請求項１２に記載されたプログラムによって暗号化されたデータの復号化プログラムであって、
あらかじめ定められたn個(nは正の整数)のうちのk個(kはk≦nである正の整数)の秘密鍵と保存されたしきい値ロジックの計算結果から、前記しきい値ロジックに対応するしきい値逆ロジックを使用して鍵を復元し、
前記復元した鍵を使用して共通鍵暗号方法によって保存された暗号化データを復号化することを特徴とするデータの復号化プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、秘密分散法を用いたセキュリティ技術に関する。
【０００２】
【従来の技術】公開鍵暗号に用いる秘密鍵のような秘密情報を保管する場合、秘密情報の紛失や破壊に対するおそれと、秘密情報の盗難のおそれがある。紛失や破壊に対しては、秘密情報のコピーを複数作ることにより対処できるが、コピーが増えると盗難に対するおそれが増加する。これらの問題の解決手段として、秘密分散法がある。その中の一つに(k,n)しきい値秘密分散法がある。これは、秘密情報sを定数項とする(k-1)次の多項式f(x)とし、
$f(x)=s+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1} \bmod r$（但し、r：素数)
分配者は、分散された秘密を持つ各秘密分散保持者i(i＝1,2,…,n)に分散情報$w_i=f(i)$を配るものである。
【０００３】この(k,n)しきい値秘密分散法は、任意のk(k≦n)個の分散された秘密情報がそろえば、秘密情報sを復元できるが、任意のk-1個までの秘密情報がそろっても秘密情報sは復元できないというものである。したがって、k-1個までの秘密情報が他人に知られても秘密情報が漏れず、n-k個まで分散情報を失っても秘密情報sを復元できるという特徴を持つ。詳しくは、A.Shamir “How to Share a Secret”,Commun.of ACM, Vol.22, No.11, pp.612 - 613, 1979に述べられている。
【０００４】
【発明が解決しようとする課題】しかし、従来の(k,n)しきい値秘密分散法を用いて、情報の暗復号化を行うには、以下の2点の問題があった。
(1)分配者が秘密情報を知ってしまう点
(2)秘密分散情報を作成する分配者機関が必要な点
本発明の目的は、安全かつ高信頼な秘密分散方法と、それを用いた暗号化方法、復号化方法を提供することであり、さらに、これらの方法を用いたデータ管理システムと、それを実現する個々の装置とそこで実行されるプログラムを提供することである。
【０００５】
【課題を解決するための手段】上記問題を解決するために、本発明では以下の手段を用いてシステムを構築した。
(1)秘密分散保持者が保有するデータ、すなわち上記分散情報を公開鍵暗号における秘密鍵とする。
(2)(k,n)しきい値秘密分散法におけるしきい値ロジック、すなわち秘密分散方法、または、秘密分散手順として、各秘密分散保持者の秘密鍵と対を成す公開鍵を用いた計算を行う。
これらの手段を用いることにより、公開情報である公開鍵のうち一つ又は複数を用いて暗復号化鍵、すなわち共通鍵暗号の共通鍵を生成して、その暗復号化鍵を用いて情報の暗号化を行い、その情報の復号化には、各分散秘密保持者のもつ秘密情報である秘密鍵のうちの、しきい値ロジック(秘密分散手順)によってきまる条件を満たす、ひとつまたは複数を用いて暗復号化鍵を復元し、復元した暗復号化鍵を用いて情報の復号化をおこなうことができる。

【０００６】従来のしきい値暗号の場合には、秘密鍵に関する情報をShamirの秘密分散法などを用いて分散する。これに対し、本発明においては、各自がもつ秘密情報は、もともと互いに独立な(無関係な)値であるが、暗号化時に利用する共通鍵暗号の共通鍵を各自の公開鍵から算出する際にしきい値ロジックを利用することにより、結果として、各自のもつ秘密情報が、情報の復号化に用いる共通鍵暗号の共通鍵を導くために必要な分散された秘密情報としての意味を持つ事になる。そのため、情報を暗号化した後に、改めて秘密情報をそれぞれに分散させる必要が無くなり、分配者機関が必要なくなる。また、それに伴って分配者が存在しないために秘密情報を知られる心配も解消される。さらに、上記公開鍵暗号として楕円曲線暗号を用いることで、処理の高速化が可能になる。

【０００７】すなわち、本発明のデータの暗号化復号化方法は、(1)暗号化する時に、公開鍵暗号方法によって、秘密鍵(d_n)と公開鍵(Q_n)とをn組(nは正の整数)準備し、少なくとも1つの公開鍵から新たな鍵を生成し、新たな鍵とn個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(kはk≦nである正の整数)を準備し、新たな鍵とn個の公開鍵を使用して、しきい値ロジックの計算を行い、暗号化されたデータとしきい値ロジックの計算結果を保存し、(2)復号化をする時に、n個の内のk個の秘密鍵と保存されたしきい値ロジックの計算結果から、しきい値ロジックに対応する値しきい値逆ロジックを使用して新たな鍵を復元し、復元した鍵を使用して共通鍵暗号方法によって保存された暗号化データを復号化することを特徴とするものである。

【０００８】さらに、本発明のデータの暗号化復号化方法は、公開鍵暗号方法は楕円曲線暗号であって、楕円曲線暗号に関係する定数(R)が暗号化データとともに保存され、復号化時に利用されることを特徴とするものである。さらに、本発明のデータの暗号化復号化方法は、公開鍵から新たな鍵を生成する時に、ハッシュ関数を使用することを特徴とするものである。さらに、本発明のデータの暗号化復号化方法は、楕円曲線暗号に関係する定数(R)は、楕円曲線のベースポイント(P)と乱数から計算され、新たな鍵は公開鍵と該乱数から計算される値のハッシュ値であり、しきい値ロジックは公開鍵と該乱数から計算される値のハッシュ値および新たな鍵を変数とする連立方程式を用いることを特徴とするものである。

【０００９】さらに、本発明のデータの暗号化復号化方法は、新たな鍵を復号する時に、秘密鍵と定数を使用した計算結果のハッシュ値をしきい値逆ロジックで用いることを特徴とするものである。さらに、本発明のデータの暗号化復号化方法は、(n-k)個以下の秘密鍵が使用不可能になった時は、残りの少なくともk個の秘密鍵を使用して保存された暗号化データを復号し、使用不可能な鍵またはすべての鍵に対して、秘密鍵と公開鍵を新たに用意し、新しい公開鍵を使用して、再度復号化されたデータの暗号化を行うことを特徴とするものである。

【００１０】また、本発明のネットワークシステムは、ネットワークに接続され、それぞれ公開鍵暗号方法の秘密鍵を保管するn個(nは正の整数)の機器と、ネットワークに接続され複数の機器のいずれからもアクセス可能であり、秘密鍵に対応するすべての公開鍵を保管するサーバとを含むネットワークシステムであって、データの暗号化を行う機器は、少なくとも1つの公開鍵から新たな鍵を生成する手段と、新たな鍵を使用して共通鍵暗号方法によってデータを暗号化する手段と、新たな鍵とn個の公開鍵を使用して、新たな鍵とn個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(kはk≦nである正の整数)の計算を行う手段と、暗号化されたデータとしきい値ロジックの計算結果をサーバに保存する手段を含み、データの復号を行う機器は、暗号化されたデータとしきい値ロジックの計算結果をサーバから読み出す手段と、秘密鍵に関係し、しきい値ロジックに対応するしきい値逆ロジックの計算に必要なk個の値を機器から得る手段と、読み出したしきい値ロジックの計算結果と得た値から、しきい値逆ロジックを使用して新たな鍵を復元する手段と、復元した鍵を使用して共通鍵暗号方法によって読み出された暗号化データを復号化する手段を含むことを特徴とするものである。

【００１１】さらに、本発明のネットワークシステムは、公開鍵暗号方法の秘密鍵を保管するn個の機器は、コンピュータ又は他の装置を介してネットワークに接続可能なICカードであることを特徴とするものである。さらに、本発明のネットワークシステムは、公開鍵暗号方法は楕円曲線暗号であって、暗号化装置において、新たな鍵生成手段は、公開鍵と乱数から計算される値のハッシュ値を新たな鍵とし、公開鍵と乱数から計算される値のハッシュ値および新たな鍵を変数としてしきい値ロジックの計算を行い、暗号化機器の保存手段は、楕円曲線暗号に関係する定数(R)を楕円曲線のベースポイント(P)と乱数から計算して暗号化データと共に保存し、復号化機器において読み出し手段は、定数を読み出し、得る手段は、秘密鍵と定数の計算結果のハッシュ値を得ることを特徴とするものである。

【００１２】さらに、本発明のネットワークシステムは、復号化機器の得る手段は、秘密鍵を持つ他の機器に定数と共に秘密鍵のハッシュ処理要求を送信し、該他の機器からハッシュ値を受信することを特徴とするものである。さらに、本発明のネットワークシステムは、機器の各々は、秘密鍵のハッシュ処理要求を受信する手段と、ハッシュ処理要求とともに送信されてきた定数と自機器内に保管している秘密鍵とを使用した計算結果のハッシュ処理を行う手段と、該ハッシュ値を該ハッシュ処理要求送信元に送信する手段とを持つことを特徴とするものである。

【００１３】また、本発明のデータの暗号化プログラムは、公開鍵暗号方法によって、秘密鍵(d_n)と公開鍵(Q_n)とをn組(nは正の整数)準備し、少なくとも1つの公開鍵から新たな鍵を生成し、新たな鍵を使用して共通鍵暗号方法によってデータを暗号化し、新たな鍵とn個の公開鍵に関係する項をもつ(k,n)しきい値ロジック(k≦nである正の整数)を準備し、新たな鍵とn個の公開鍵を使用して、しきい値ロジックの計算を行い、暗号化されたデータとしきい値ロジックの計算結果を保存することを特徴とするものである。

【００１４】また、本発明は、上記データの暗号化プログラムによって暗号化されたデータの復号化プログラムであって、あらかじめ定められたn個(nは正の整数)のうちのk個(kはk≦nである正の整数)の秘密鍵と保存されたしきい値ロジックの計算結果から、しきい値ロジックに対応するしきい値逆ロジックを使用して鍵を復元し、復元した鍵を使用して共通鍵暗号方法によって保存された暗号化データを復号化することを特徴とするものである。

【００１５】

【発明の実施の形態】(1)システムの構成

本発明による一実施例を図面を用いて説明する。図1は、本発明を用いて構成したデータ管理システムの概略構成図であり、ファイル111が管理されているファイルサーバ102と、秘密鍵d_1 107が記憶された部長Aのコンピュータ103と、秘密鍵d_2 108が記憶された課長Bのコンピュータ104とがネットワーク101を介して接続されている。また、課長Bは秘密鍵d_3 109が記憶されたICカードB105を、秘書Cは秘密鍵d_4 110が記憶されたICカードC106を保有しているものとする。

【００１６】ここで、ネットワーク101は汎用ネットワークであり、例えばLANである。ファイルサーバ102及びコンピュータ103,104はパーソナルコンピュータ、ワークステーションなどの計算機であって、メモリ、CPU、通信インターフェイスをもつ。ICカード105,106は、メモリ、CPU、メモリ内のデータを入出力するためのインターフェイスをもつ。ファイルサーバとコンピュータ及びコンピュータ間のデータ転送は、ネットワーク1010が採用するプロトコル、例えばTCP/IPにしたがって行われる。

【００１７】このシステムでは後述するように、ビット長の長い、例えば160ビットの整数演算を行う。従って、コンピュータ、ICカードはこの整数演算を行うために専用のプロセッサを含んでも良いし、ビット長の長い整数を通常のビット長(例えば32ビット)に分割して演算を行うロジック（すなわちソフトウェア、ファームウェアといったRAM,ROMやEPROMに書き込まれたプログラム）を含んでも良い。

【００１８】まず、システム管理者は公開鍵暗号のアルゴリズムを決定する。本実施例では、公開鍵暗号として楕円曲線暗号を使用するため、システムごとにどの楕円曲線を使用するか、より具体的には、利用する楕円曲線の種類(パラメータ)およびベースポイント、をシステム管理者が決定し、システム内のメンバー(本実施例では計n個の、コンピュータとICカード)には、秘密鍵と公開鍵をペアで生成するソフトウェアが配布される。各メンバー$_n$は鍵を生成して秘密鍵(d_n)を自メモリ内に保管し、公開鍵(Q_n)を公開する。公開鍵は、たとえば、ファイルサーバ102に保存される。

【００１９】更にシステム内のメンバーは後述の処理を行うために、ハッシュ関数(すなわち、メッセージダイジェストを求める関数)、ファイル暗号化・復号化、しきい値ロジックの計算、乱数生成などを行うソフトウェアをもつ。図1の例は、1台のファイルサーバ、2台のコンピュータ、および、2枚のICカードを含むが、それらの装置の数は限定されない。ICカードは使用されなくても良い。

【００２０】(2)ファイルの暗号化：例1

オリジナルのファイルをもつコンピュータがマルチメディアデータなどからなるファイルの暗号化を行い、暗号化されたファイルをファイルサーバ102にネットワーク経由で送る例を考える。

【００２１】ファイルサーバは暗号化されたファイル（暗号化されたデータ）をファイル111に格納する。ここでは、部長Aのコンピュータ103がファイルの暗号化を行うと仮定する。まず、ファイルの暗号化を行う方法を説明する。その詳細なフローを示したのが図2である。以下、この図2に従って説明する。

【００２２】ステップ201：開始。

ステップ202：部長Aのコンピュータ103において乱数kを生成する。

乱数kはシステムで使用している楕円曲線のベースポイントの位数より小さい0以上の整数であり、秘密鍵と同じビット長(例えば160ビット)である。

ステップ203：秘密鍵d_1 107に対する公開鍵Q_1と乱数kを用いて楕円曲線上の演算、具体的にはスカラー倍演算を行い、演算後の結果(x_1, y_1)を得る。

ステップ204：秘密鍵d_2 108に対する公開鍵Q_2と乱数kを用いて楕円曲線上の演算を行い、演算後の結果(x_2, y_2)を得る。

ステップ205：秘密鍵d_3 109に対する公開鍵Q_3と乱数kを用いて楕円曲線上の演算を行い、演算後の結果(x_3, y_3)を得る。

ステップ206：秘密鍵d_4 110に対する公開鍵Q_4と乱数kを用いて楕円曲線上の演算を行い、演算後の結果(x_4, y_4)を得る。

前述の通り、公開鍵Q_1～Q_4は公開されているので誰でも入手する事ができる。公開鍵Q_1はxy座標の形で表され、x, yはそれぞれ楕円曲線が定義されている体の位数より小さい0以上の整数として表す事ができる。

ステップ207：ステップ203の演算結果のx_1にハッシュ関数hを作用させて、ハッシュ値$h(x_1)$を得る。
ステップ208：ステップ204の演算結果のx_2にハッシュ関数hを作用させて、ハッシュ値$h(x_2)$を得る。
ステップ209：ステップ205の演算結果のx_3にハッシュ関数hを作用させて、ハッシュ値$h(x_3)$を得る。
ステップ210：ステップ206の演算結果のx_4にハッシュ関数hを作用させて、ハッシュ値$h(x_4)$を得る。
ステップ211：ステップ207で求めたハッシュ値$h(x_1)$を暗復号化鍵として、オリジナルのファイル、すなわちデータMを暗号化し、結果として暗号化されたデータCを得る。
【００２３】ステップ211で行う暗号化には、暗号化と復号化に同じ鍵を使用する共通鍵暗号方法を採用する。代表的にはDES(Data Encryption Standard)であるが、その他の共通鍵暗号方法でも良い。ステップ207～210の一方向性関数は、共通鍵暗号方法で用いる鍵長以上のメッセージダイジェスト値を生成する関数であれば、なんでも良い。代表的にはSHA-1である。ここで用いる共通鍵暗号方法及びハッシュ値はより安全性が高いものが良い。ステップ207～210では同一のハッシュ関数を使用しても良いし、複数の異なるハッシュ関数を使用しても良い。ハッシュ値の長さが共通鍵暗号化の鍵長より長い場合は、ハッシュ値を部分的に使用する。SHA-1のハッシュ値長は160ビット、DESの鍵長は56ビットであるが、この場合ハッシュ値の先頭56ビット又は末尾56ビットなど、あらかじめ決めた任意の56ビットを抜き出して、鍵として使用する。
【００２４】ステップ212：しきい値ロジックに従い、計算を行う。ここでは、そのロジックの一例として、秘密鍵d_1 107のみを用いて復号化することができ、さらに秘密鍵d_2 108、秘密鍵d_3 109、秘密鍵d_4 110の3つ鍵のうち2つがそろった時に復号化できるロジックを用いることとする。しきい値ロジックへの入力値を、上記ステップ207から210までに計算したハッシュ値$h(x_1)$、$h(x_2)$、$h(x_3)$、$h(x_4)$、及び、公開鍵Q_1のx座標とする。この時、以下の4元連立方程式を計算して出力f_1、f_2を得る。

$$f_1 = a_1 h(x_1) + a_2 h(x_2) + a_3 h(x_3) + a_4 h(x_4)$$
$$f_2 = b_1 h(x_1) + b_2 h(x_2) + b_3 h(x_3) + b_4 h(x_4)$$

但し、a_I,b_i ($i=1,2,3,4$)はQ_1のx座標から算出される定数であって、例えば秘密情報分散法で良く使用されるVandermonde Matrixと呼ばれる係数行列である。
【００２５】ステップ213：楕円曲線上のベースポイントPと乱数kから楕円曲線上の演算を行い、演算後の結果$R(x,y)$を得る。
ベースポイントP及び演算結果Rは公開鍵と同じ形式、すなわちビット長の長い0以上の整数であり、x,y座標で表される。ベースポイントPは楕円曲線暗号の鍵生成ソフトウェアとともに各メンバーに配布されても良いし、公開鍵と一緒に公開されても良い。
ステップ214：出力処理として、ステップ211で計算した暗号文データCと、ステップ213で計算したRと、ステップ212で計算したf_1とf_2を出力する。
ステップ215：終了。
【００２６】以上の処理で、コンピュータ103は、生成された暗号化データCをファイルサーバ102へ送信し、ファイル111にストアする。ステップ214で出力されたデータR,f_1,f_2も暗号化データcと対応づけて保管される。R,f_1,f_2は暗号化データCとともにファイル111に保管されても良いし、別の公開データとともにネットワークを介して参照可能である場所に保管されても良い。
【００２７】上述のハッシュ関数、および公開鍵とハッシュ関数の関係、ハッシュ値と暗号化鍵との対応、共通鍵暗号方法、しきい値ロジックの係数行列はシステムで1つに定めても良いし、暗号化されるデータごとに定めても良い。前者の場合はこれらは図2に示したプログラム内に組み込まれても良い。後者の場合それらの情報は、R,f_1,f_2と同様に暗号化データCとリンクされた形で、誰でも参照可能な場所に保管される。
【００２８】図2ではステップ203～210が並列した形で描かれているが、これはしきい値ロジックと公開鍵Qの関係を明白にするためである。ファイルの暗号化を行うコンピュータのプロセッサが1つである場合、これらの処理はシリアライズされる。以上のステップは、公開鍵と図2のステップを実行するコンピュータ内で生成する乱数とを用いるので、他のコンピュータでも実行可能である。
【００２９】(3)ファイルの復号化：例1
前節の例1で暗号化されたファイル(暗号化データc)を復号化する方法を説明する。例1では、ファイルの暗号化鍵として$h(x_1)$、すなわち、秘密鍵d_1にのみに関係する値を使用している。したがって秘密鍵d_1を知る人(ここでは部長A)は、単独でファイルの復号化を行う事ができる。秘密鍵d_1を知らない場合は前述のしきい値ロジックに従って複数の秘密鍵所有者が合意しないと(ここでは2人)と、ファイルの復号化を行う事はできない。両方の復号化方法を説明する。
【００３０】(A)部長Aによるファイルの復号化
部長Aの持つ秘密鍵d_1 107を用いたファイルの復号化方法を説明する。以下、図3に従って説明する。
【００３１】ステップ301：開始。
ステップ302：コンピュータ103は、コンピュータ103の通信機能を用いて、ネットワーク101を介してファイルサーバ102又は、他の誰でもアクセス可能な場所に記憶されているファイル111からデータRを得る。
ステップ303：ステップ302で得たデータRと、部長Aのコンピュータ103の記憶装置に記憶してある秘密鍵d_1 107を用いて、以下の楕円曲線上の演算$(x,y)=d_1 R$を実行する。この演算によって得られた値は、以下の関係から(x_1,y_1)となることがわかる。

$(x,y)=d_1R=d_1(kP)=k(d_1P)=kQ_1=(x_1,y_1)$
ステップ304：演算結果x_1にハッシュ関数hを作用させ、ファイルを暗号化した暗復号化鍵$h(x_1)$を復元する。
ステップ305：ステップ304で復元した暗復号化鍵$h(x_1)$を用いて暗号化されたデータCを読み出して復号化し、データMを得る。
ステップ306：終了。
【００３２】ステップ304で用いるx_1のためのハッシュ関数hは、図2で説明した暗号化時に使用した関数と同じものである。又、ステップ305は、図2のステップ211で暗号化したデータを復号化できる方法を用いて行う。
以上のステップは、部長Aのコンピュータ103中のCPUが、同じくコンピュータ103中の記憶装置に格納されているプログラムを実行することで実現されるものである。
【００３３】(B)しきい値制御によるファイルの復号化
ファイルの暗号化を行う際に用いたしきい値ロジックの逆ロジックを用いることにより、秘密鍵$d_2$108、秘密鍵$d_3$109、秘密鍵$d_4$110の3つ鍵のうち2つがそろった時の復号化方法を説明する。その一例として、課長BがICカードB105を携帯したまま不在中であるとし、ファイルの復号化を依頼された秘書CがICカードC106と、課長Bのコンピュータ104を用いてファイルを復号化する方法を説明する。以下、図4に従って説明する。
【００３４】ステップ401：開始
ステップ402：コンピュータ104が、ネットワーク101を介してファイルサーバ102のファイル111又は誰でもアクセス可能な場所からデータRとf_1とf_2を得る。
ステップ403：コンピュータ104は、ステップ402で得たデータRと、課長Bのコンピュータ104中の秘密鍵$d_2$108を用いて、楕円曲線上の演算$(x,y)=d_2R$を実行する。この演算によって得られた値は、ステップ303と同様の関係から(x_2,y_2)となる。
ステップ404：コンピュータ104は、演算結果x_2にハッシュ関数hを作用させ、ハッシュ値$h(x_2)$を得る。
【００３５】ステップ405：ステップ402で得たデータRと、秘書CのICカード106に記憶してある秘密鍵$d_4$110を用いて、楕円曲線上の演算$(x,y)=d_4R$を実行する。この演算によって得られた値は、ステップ303と同様の関係から(x_4,y_4)となる。
ステップ406：演算結果x_4にハッシュ関数hを作用させ、ハッシュ値$h(x_4)$を得る。
ステップ407：104ステップ402で得たf_1とf_2、ステップ404で得た$h(x_2)$、IC106ステップ406の実行結果$h(x_4)$、さらに公開情報である公開鍵Q_1を用いてしきい値逆ロジックからファイルを暗号化した鍵$h(x_1)$を復元する。
【００３６】以上の説明において、ステップ403,404,407の演算は課長Bのコンピュータ104中のCPUが、同じくコンピュータ104中の記憶装置に格納されているプログラムを実行することで実現される。ステップ405,406の演算はICカード106中のプロセッサが、コンピュータ104からデータRを受け取り、ICカード106中に格納されている秘密鍵d_4を用い、ICカード106中に格納されているプログラムを実行することで実現される。以上のステップでは、秘密鍵はそのままの形で秘密鍵が記憶されているコンピュータやICカードの外へ送出されないほうが良い。秘密鍵がネットワーク上をデータとして送信されると盗聴される等の危険が増すためである。従って、上記ステップ403、404及びステップ405,406は、それぞれ秘密鍵を保管するコンピュータ又はICカード上でなされるものとしている。
【００３７】これらのステップを行うコンピュータ又はICカード(本例ではICカード106)がファイル復号を行うコンピュータ(本例ではコンピュータ104)と異なる場合は、さらに次のステップを行うことにより、上記危険を回避することができる。
【００３８】ステップ410：コンピュータ104はRとともにハッシュ処理要求をICカード106に送る。
ステップ411：コンピュータ104はハッシュ値$h(x_4)$をICカード106から受け取る。
【００３９】なお、ICカード106がステップ405,406を実行している間、コンピュータ104はwait状態となるかあるいは他の処理を実行する(通常の分散処理と同じ)。ここでR及びハッシュ値はネットワーク、又は/および、コンピューターICカード間インターフェースを経由して送信される。ステップ410ではRとともにステップ406で使用されるハッシュ関数が一緒に送られても良い。ステップ404、406で用いるハッシュ関数は図2の暗号化に使用したハッシュ関数と同じである。
【００４０】ここで、さらにしきい値逆ロジックを説明する。しきい値逆ロジックとは、しきい値ロジックが秘密を分散する方法であるのに対し、分散された秘密から、元の秘密を復元する方法、手順のことをいう。しきい値ロジックで用いた以下の式はf_1とf_2と公開鍵Q_1(又はa_i,b_iの係数行列)が与えられた時、未知数を$h(x_1)$、$h(x_2)$、$h(x_3)$、$h(x_4)$とする4元連立方程式となる。

$$f_1=a_1h(x_1)+a_2h(x_2)+a_3h(x_3)+a_4h(x_4)$$
$$f_2=b_1h(x_1)+b_2h(x_2)+b_3h(x_3)+b_4h(x_4)$$

ここで、$h(x_2)$、$h(x_4)$が得られれば、未知数が$h(x_1)$、$h(x_3)$の2つとなり、2元連立方程式から$h(x_1)$を求めることが可能となる。
【００４１】ステップ408：暗号化されたデータCをファイルサーバ102から読み出しステップ407で復元した暗復号化鍵$h(x_1)$を用いて暗号化されたデータCを復号化し、データMを得る。
ステップ409：終了。
【００４２】図4ではステップ403～406,410,411が並列する処理として描かれているが、これはハッシュ値としきい値ロジックの関係を明白にするためである。なお、この実施例は、たとえば、課長BのPC108が壊れて秘密鍵

$d_2$108が読み出せなくなった場合にICカード105を使ってファイルの復号化を行う場合にも、上記実施例での秘密鍵d_2をd_3と置き換えることで適用できる。以上の説明では、復号をコンピュータ104で実行するものとしたが、これに限定はされず、必要なデータを受け取れれば、他のコンピュータたとえばファイルサーバ102上でも実現できる。

【００４３】(4)ファイルの暗号化：例2

例1で説明したファイルの暗復号化処理は、秘密鍵$d_1$107のみを用いて復号化することができ、さらに秘密鍵$d_2$108、秘密鍵$d_3$109、秘密鍵$d_4$110の3つ鍵のうち２つがそろった時に復号化できて一つでは復号化できないロジックであるが、しきい値ロジックを変更することにより、様々なしきい値制御が可能となる。例えば、上記実施例では、ファイルの暗号化を行う際に用いた暗号化鍵は公開鍵Q_1から導出されたハッシュ値$h(x_1)$であったが、4つの公開鍵から導出された値の部分情報の和のハッシュ値$h(x_1||x_2||x_3||x_4)$を暗号化鍵として用い、この値をしきい値ロジックにより秘密分散させればよい。||は結合を表す演算子であり$x_1||x_2||x_3||x_4$はx_1～x_4のビット列を単に連結した長いビット列となる。

【００４４】以下に例として、(2,4)しきい値秘密分散ロジックを示す。

$g_1=s_1h(x_1||x_2||x_3||x_4)+s_2h(x_1)+s_3h(x_2)+s_4h(x_3)+s_5h(x_4)$

$g_2=t_1h(x_1||x_2||x_3||x_4)+t_2h(x_1)+t_3h(x_2)+t_4h(x_3)+t_5h(x_4)$

$g_3=u_1h(x_1||x_2||x_3||x_4)+u_2h(x_1)+u_3h(x_2)+u_4h(x_3)+u_5h(x_4)$

上記演算式において、s_i,t_i,u_i(i＝1,2,3,4,5)を公開鍵Q_i(i＝1,2,3,4)から算定される定数としておくと、未知数が$h(x_1||x_2||x_3||x_4)$、$h(x_1)$、$h(x_2)$、$h(x_3)$、$h(x_4)$の5つ、方程式3つの5元連立方程式となる。ここで、各秘密鍵のうち少なくとも2つがそろえば未知数が3つとなり、方程式が3つの3元連立方程式となり、これを解くことにより、暗号化鍵$h(x_1||x_2||x_3||x_4)$を得ることができる。この方法では、上述のネットワークシステムにおいてたとえば部長一人の秘密鍵でも暗復号化鍵を得ることができないシステムを構成することができる。すなわち、この例2では、4人のうちの任意の2人がそろった時に復号できることになる。

【００４５】暗号化のプロセスを図5に示す。ほとんどのステップは図2に示したプロセスと同じである。しかし、ファイルの暗号化を行うステップ221aで、ステップ203～206で計算されたすべての値x_1～x_4に関係する鍵$h(x_1||x_2||x_3||x_4)$を使用する事が図2とは異なる。

【００４６】(5)ファイルの復号化：例2

図5のプロセスにしたがって暗号化された暗号文Cは図4及び(3)(B)の節で説明した方法と同じ方法で復号化される。ただし、ステップ407で、しきい値逆ロジックにより復元されるのは$h(x_1||x_2||x_3||x_4)$であり、ステップ408の復号化に使用される鍵も$h(x_1||x_2||x_3||x_4)$である。一般には、n個の秘密鍵のうちn以下のk個の秘密鍵が集まった時にファイルを暗復号化できて、k-1個以下の秘密鍵だけではファイルの暗復号化ができないようにしきい値ロジックを構成することが可能である。これによって、システムの信頼性と安全性とを確保することができる。

【００４７】(6)鍵の更新

鍵の紛失や破壊時の対策法を、上記実施例の場合を一例として説明する。上記実施例では、4つの鍵を用いたしきい値ロジックによる制御を示した。しかし、この4つの鍵のうち、任意の2個の鍵が紛失又は破壊されたとしても、ファイルは復号化は可能である。そのため、鍵が一つでも紛失又は破壊された時、直ちに残りの3つの鍵のいずれかを用いて一時的にファイルを復号化する。44102次に紛失又は破壊された鍵のかわりに新たに公開鍵・秘密鍵を生成する。この時にすべての(4つの)鍵を生成し直しても良い。この新しい鍵の組を使用して再度ファイルの暗号化を行う。

【００４８】この方法により、(k,n)しきい値ロジックを使用している場合(n-k)個までの鍵の紛失・破壊に対しては暗号文の復号化ができなくなる危険を回避できる。本発明は、たとえば高い信頼性と安全性とが要求される電子商取引のような分野に応用することができるという効果もある。

【００４９】(7)変形例

上述の例では、4人が秘密鍵を持つ場合を示したが、2人以上で秘密鍵を持つ場合に本発明は適用できる。上述の例では楕円曲線上の有理点の生成する群を利用した楕円曲線暗号を使用しているが、他の群構造を利用した暗号であっても良い。例えば超楕円曲線のヤコビアン群や、C_{AB}曲線のヤコビアン群、またはそれらの部分群、あるいは、整数環の部分群を利用した暗号であっても良い。この変形例に示したような、群構造を利用する公開鍵暗号系であれば、前記システム管理者はどの群を利用するかを、あらかじめ決めることになる。

【００５０】

【発明の効果】上述のように本発明によれば、秘密情報の分配処理が存在しないため、分配者に秘密情報を見られることもなく、また、ネットワークにおける分配者機関も必要としなくなる。したがって、安全で信頼性の高い秘密分散方法と、それを用いた暗号化方法、復号化方法と、さらに、それらを用いたデータ管理システムを実現することができる。

【図面の簡単な説明】

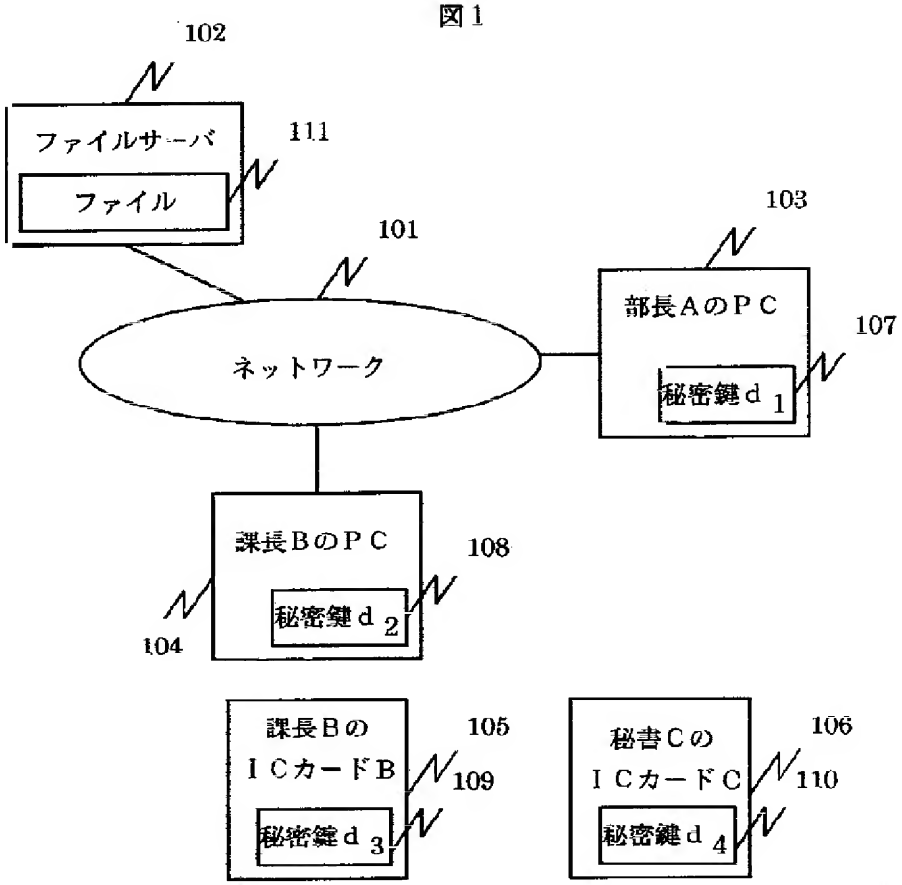
【図１】本発明による、ネットワークシステムの一例を示す図である。

【図２】しきい値ロジックを用いてファイルを暗号化する場合の一例を示すフローチャートである。

【図３】図1におけるネットワーク上で、部長Aが秘密鍵$d_1$107を用いてファイルを復号化する場合のフローチャートである。
【図４】図1におけるネットワーク上で、秘書Cが秘密鍵$d_2$108と秘密鍵$d_4$110をもちいてファイルを復号化する場合のフローチャートである。
【図５】しきい値ロジックを用いてファイルを暗号化する場合の他の例を示すフローチャートである。
【符号の説明】
101…ネットワーク、
102…ファイルサーバ、
103…部長Aのコンピュータ、
104…課長Bのコンピュータ、
105…課長BのICカードB、
106…秘書CのICカードC、
107…秘密鍵d_1、
108…秘密鍵d_2、
109…秘密鍵d_3、
110…秘密鍵d_4、
111…ファイル。

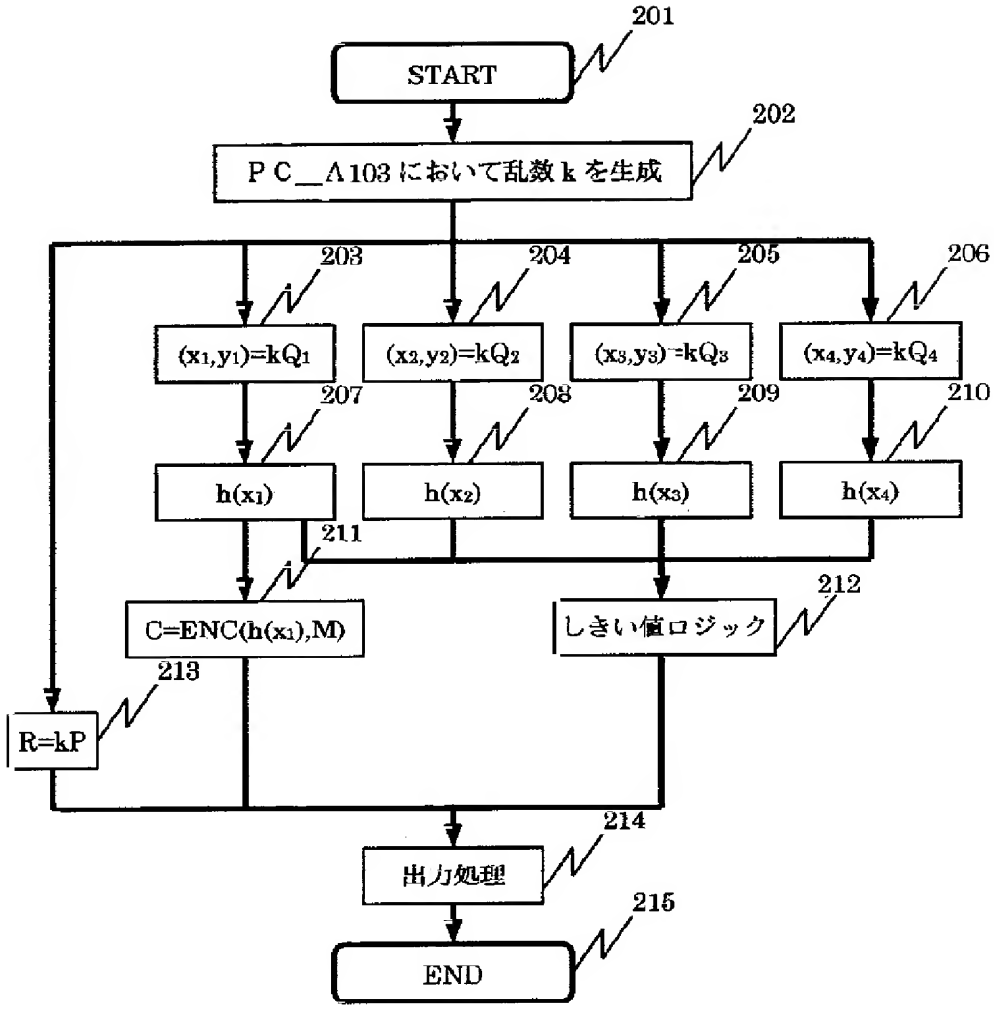
【図１】

図１



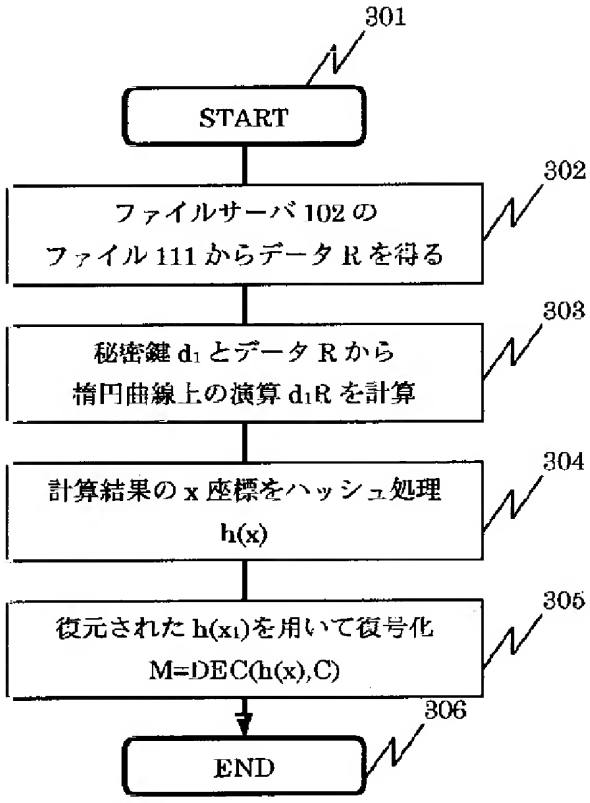
【図２】

図２


201
START
202
ＰＣ＿Ａ103において乱数ｋを生成
203
204
205
206
(x1,y1)=kQ1
(x2,y2)=kQ2
(x3,y3)=kQ3
(x4,y4)=kQ4
207
208
209
210
h(x1)
h(x2)
h(x3)
h(x4)
211
212
C=ENC(h(x1),M)
しきい値ロジック
213
R=kP
214
出力処理
215
END

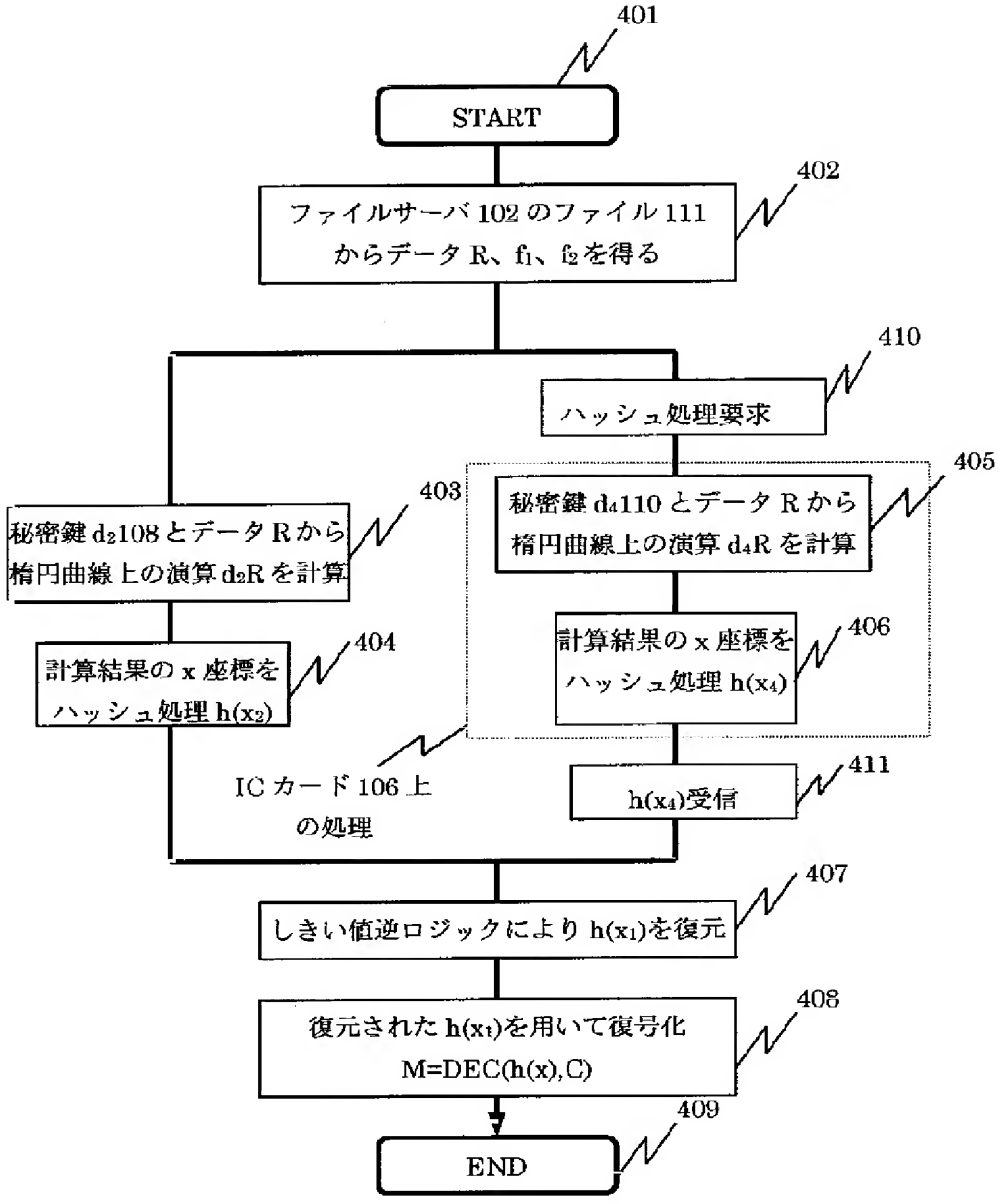
【図３】

図３


301
START
302
ファイルサーバ102の
ファイル111からデータRを得る
303
秘密鍵 d_1 とデータRから
楕円曲線上の演算 d_1R を計算
304
計算結果のx座標をハッシュ処理
h(x)
305
復元された $h(x_1)$ を用いて復号化
M=DEC(h(x),C)
306
END

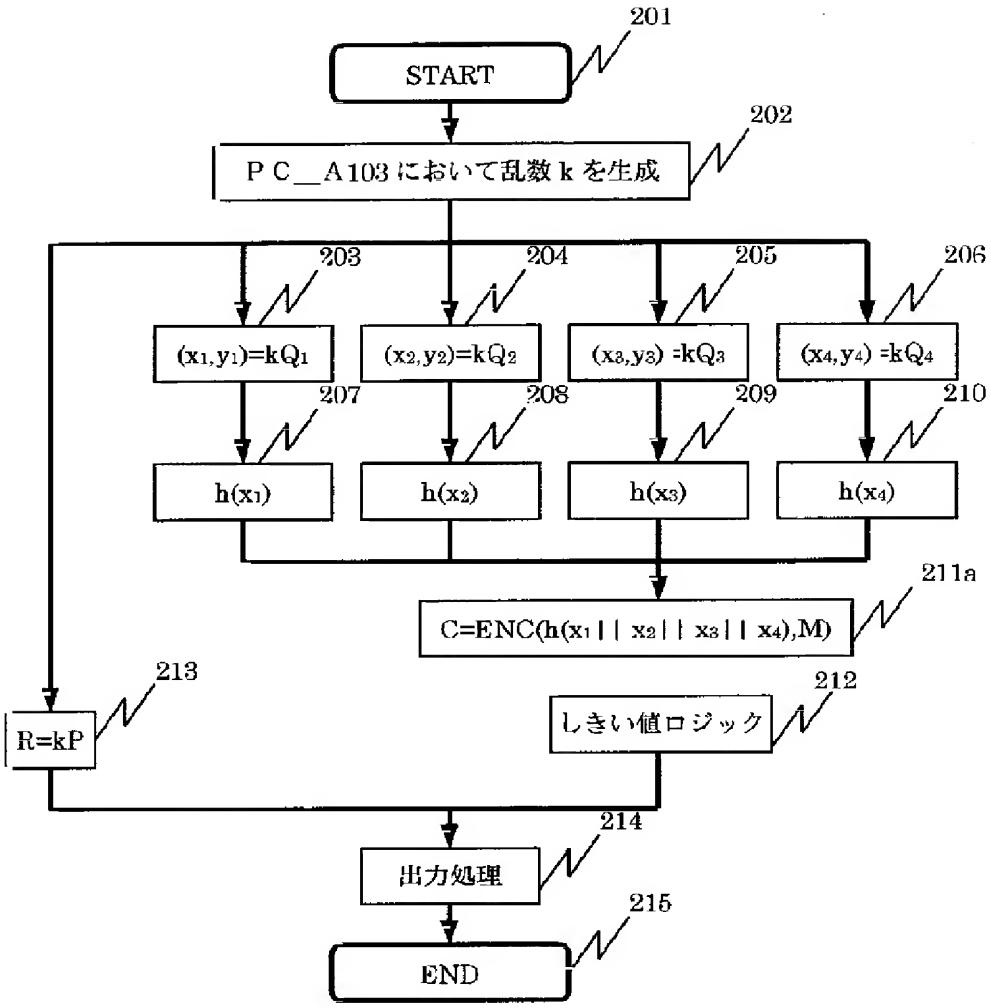
【図４】

図４


401
START
402
ファイルサーバ102のファイル111
からデータR、f1、f2を得る
410
ハッシュ処理要求
405
秘密鍵d4110とデータRから
楕円曲線上の演算d4Rを計算
403
秘密鍵d2108とデータRから
楕円曲線上の演算d2Rを計算
404
計算結果のx座標を
ハッシュ処理h(x2)
406
計算結果のx座標を
ハッシュ処理h(x4)
ICカード106上
の処理
411
h(x4)受信
407
しきい値逆ロジックによりh(x1)を復元
408
復元されたh(x1)を用いて復号化
M=DEC(h(x),C)
409
END

【図５】

図５


201
START
202
ＰＣ＿Ａ103において乱数ｋを生成
203
204
205
206
(x1,y1)=kQ1
(x2,y2)=kQ2
(x3,y3)=kQ3
(x4,y4)=kQ4
207
208
209
210
h(x1)
h(x2)
h(x3)
h(x4)
211a
C=ENC(h(x1||x2||x3||x4),M)
213
R=kP
212
しきい値ロジック
214
出力処理
215
END